Upper bounds on the tradeoff between loss and error rates in non-degenerate quantum error correcting codes

Peter P. Rohde[1]

[1]Centre for Quantum Computer Technology, Department of Physics
University of Queensland, Brisbane, QLD 4072, Australia
e-mail: rohde@physics.uq.edu.au
URL: http://www.physics.uq.edu.au/people/rohde/

(Dated: May 23, 2006)

A recent study [Rohde et al., quant-ph/0603130 (2006)] of quantum error correcting codes specifically targeting qubit loss found they generally have the undesirable effect of magnifying depolarizing noise. This results in a tradeoff between these two error types. If we desire high loss tolerance, our tolerance against depolarizing noise is reduced, and vice versa. In this paper we expand on this notion by deriving an upper bound on the tradeoff between qubit loss and depolarizing noise tolerance for a general class of non-degenerate codes. Our approach employs a variation of the well-known quantum Hamming bound to establish a relationship between the number of loss and depolarizing errors a code of given size can correct. We then consider the situation where we require the effective error probability on encoded qubits to satisfy some upper bound, and examine the tradeoff between tolerable physical loss and error rates.

PACS numbers: 03.67.Pp,03.67.-a,03.67.Lx

Quantum computing offers the potential to solve computational problems intractable on classical computers. One of the great challenges facing the development of quantum computers is decoherence, a problem which affects all known quantum computing architectures. This has motivated much research into fault-tolerant quantum computing [1, 2]. The most fundamental building blocks in fault-tolerant quantum circuits are quantum error correcting codes (QECC's) [3, 4, 5, 6], which encode logical qubits in such a way as to be able to tolerate some number of physical errors.

Broadly speaking there are two main classes of errors: *located* and *unlocated* errors. A located error occurs when it is known which qubit has been affected. This includes qubit loss [13], which we consider here. An unlocated error on the other hand is one which could have affected *any* qubit, and we have no knowledge of which one. This might arise when a multi-qubit state passes through a noisy channel where each individual qubit is independently subject to random Pauli errors. In this paper we use the terms located/unlocated and loss/depolarization interchangeably.

Traditionally QECC's have focused on correcting the later type of error. Specifically, most existing codes aim to protect against unlocated depolarizing noise, where qubits are randomized with some probability. Recently, however, especially with the advent of photonic quantum computing architectures [7, 8], several codes have been suggested for dealing specifically with located errors in the form of qubit loss [9, 10]. It has recently been shown [11] that these loss-tolerant codes are plagued by the problem that they amplify depolarizing noise. Since scalable quantum computing requires tolerance against both error types, this fundamentally limits the level of loss-tolerance these schemes can offer and presents us with a tradeoff between the degree of each type of noise we can tolerate.

In this paper we generalize this notion and derive an upper bound on the tradeoff relationship between loss and depolarizing errors. We specifically consider the class of non-degenerate codes which jointly protect against qubit loss and depolarizing noise. We begin by reviewing the notion of a non-degenerate code and the quantum Hamming bound, which places an upper bound on how many unlocated depolarizing errors such a code can correct. We then generalize this bound to the case where both located and unlocated errors occur. The modified bound enforces a tradeoff between the number of each of these types of error a code of given length can correct. Finally we consider how this relationship affects tolerable error and loss probabilities.

Non-degenerate quantum error correcting codes: In general, quantum error correction is a three stage process (see Fig. 1). The first stage is an encoding operation which takes a k qubit logical state and encodes it into an n qubit codeword, where $n > k$. Second, the encoded state undergoes some noise process $\mathcal{E}$. Finally, we apply a recovery operation $\mathcal{R}$ which aims to recover the initial uncorrupted codeword. For successful recovery we require that $(\mathcal{R} \circ \mathcal{E})(|\psi\rangle) \propto |\psi\rangle$, where $|\psi\rangle$ is the codeword.

A non-degenerate code is one for which every correctable error maps the codeword to an orthogonal state. Thus, for two correctable errors $\hat{U}_i$ and $\hat{U}_j$ acting on codeword $|\psi\rangle$, we require that $\langle\psi|\hat{U}_i^\dagger \hat{U}_j|\psi\rangle = \delta_{ij}$.

The quantum Hamming bound: The quantum Hamming bound is an inequality that holds for non-degenerate QECC's, which places an upper bound on how many errors a code of given size can correct. We begin by reviewing the construction of this bound. Suppose our code can correct up to t unlocated depolarizing errors. There are $\sum_{i=0}^{t} \binom{n}{i} 3^i$ distinct error configurations

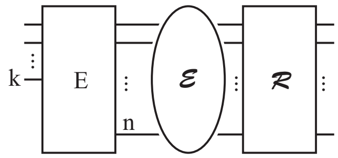

FIG. 1: The three stages of quantum error correction. First an encoding operation is applied which transforms a k qubit logical state to an n qubit codeword. The codeword undergoes some noise process $\mathcal{E}$. Finally we apply a recovery operation $\mathcal{R}$ which aims to recover the original codeword.

that may occur. The 3^i term arises from the fact that at every location there are three non-identity Pauli errors that may occur – X, Y and Z. For a non-degenerate code we require that each distinct correctable error configuration map the codeword to an orthogonal state. For this to be possible it is required that the codeword Hilbert space, which has dimensionality 2^n, be at least as large as the Hilbert space spanned by the set of correctable errors, which has dimensionality $\sum_{i=0}^{t}\binom{n}{i}3^i 2^k$. Thus follows the quantum Hamming bound,

$$\sum_{i=0}^{t}\binom{n}{i}3^i 2^k \leq 2^n. \qquad (1)$$

Interestingly, this bound does not make any assumptions about the nature of the encoding or recovery operations. Instead it is based purely on a packing argument. While the Hamming bound does not cover degenerate quantum codes, of which there are many examples, it provides some insight into the behavior of QECC's in general – to date no known codes violate the Hamming bound [1].

The generalized quantum Hamming bound: The quantum Hamming bound assumes unlocated depolarizing errors. We now modify this bound to accommodate for codes which jointly protect against both unlocated and located depolarizing errors. The new bound is

$$4^{t_l}\sum_{i=0}^{t_u}\binom{n-t_l}{i}3^i 2^k \leq 2^n \qquad (2)$$

for a non-degenerate code which tolerates up to t_u unlocated and t_l located errors. The construction of this inequality follows the same reasoning as previously, with two main differences. First, we have introduced an additional term corresponding to the located errors. This term lacks both the summation and binomial coefficient. This is because the number and location of these errors is always known. When t_l located depolarizing errors occur, there are 4^{t_l} distinct error configurations, since the depolarizing process contains four components – I, X, Y and Z [14]. Second, unlocated errors only act on the remaining $n-t_l$ qubits that were not affected by located errors. This is justified by the fact that if a qubit first suffers an error and is then lost, the initial error is redundant.

There is one caveat associated with this bound – it holds for a *particular* configuration of located errors. More precisely, bounds of the form of Eq. 2 must simultaneously hold for *every* distinct located error configuration. In general this represents a tightening of the bound. However, if we make certain assumptions about the symmetry of codes then Eq. 2 may represent a saturable upper bound. Specifically, if we restrict ourselves to codes whose ability to recover from located errors is independent of their location then these simultaneous bounds reduce to a single bound of the form shown in Eq. 2. Of course, in either case Eq. 2 represents an upper bound, but it will be insaturable in cases where this extra symmetry requirement does not hold.

This bound enforces a tradeoff between the maximum number of located and unlocated errors a non-degenerate code can correct. Upon inspection we see that well constructed codes ought to be able to correct more located errors than unlocated ones, as one expects. This owes to the additional classical information we have at our disposal in the case of located errors, which assists in the recovery operation [12].

It is insightful to consider the limiting behavior of this modified bound. In the limit where no located errors have occurred, the bound simply reduces to the original quantum Hamming bound, as expected. In the opposing limit, where *only* located errors occur, the inequality reduces to $t_l \leq (n-k)/2$. This bound reaffirms the well-known no-cloning limit and represents an intuitive upper bound [15]. The tradeoff relationship between located and unlocated errors is shown in Fig. 2. Roughly speaking, an optimal non-degenerate QECC can correct around twice and many located as unlocated errors, with a linear tradeoff between the two.

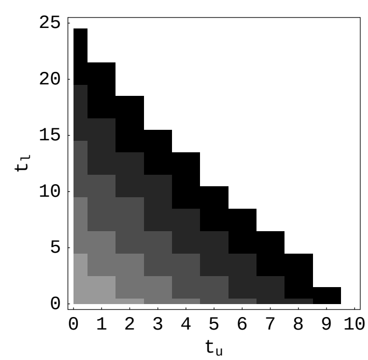

FIG. 2: Tradeoff relationship between the number of located and unlocated errors an optimal code can recover from according to the generalized quantum Hamming bound, for $n=50$ (black), $n=40$, $n=30$, $n=20$ and $n=10$ (light gray) codes.

Error probability tradeoffs: We now turn our attention to the tradeoff between located and unlocated errors in terms of error probabilities, which are a more useful quantity to deal with since they characterize physical channels.

Suppose our codewords are subject to a noisy channel characterized by depolarizing [16] probability p and loss probability ε acting independently on every physical qubit. Then the probability of a particular number of located and unlocated errors occurring is

$$r(t_l, t_u) = \binom{n}{t_l} \varepsilon^{t_l} (1-\varepsilon)^{n-t_l} \binom{n-t_l}{t_u} p^{t_u} (1-p)^{n-t_l-t_u}. \tag{3}$$

A code can only recover from this set of errors if $\{t_l, t_u\}$ satisfies the generalized Hamming bound. We define the binary function $H(t_l, t_u)$, which equals 1 when the generalized Hamming bound is satisfied, otherwise 0. Suppose we require that the probability of an unsuccessful recovery operation be upper bounded by p'. Summing over the probabilities of all ways in which unrecoverable errors may occur, we obtain

$$p' \geq 1 - \sum_{t_l, t_u} r(t_l, t_u) H(t_l, t_u). \tag{4}$$

For a given channel, characterized by p and ε, we are interested in whether this bound is satisfied. This is plotted in Fig. 3 for various codelengths n.

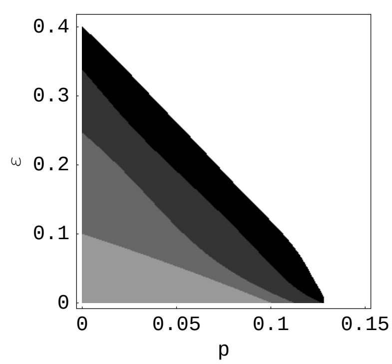

FIG. 3: Tradeoff relationship between located and unlocated error probabilities for $n = 50$ (black), $n = 20$, $n = 5$ and $n = 1$ (light gray) codes, where the effective error rate is bounded by $p' = 0.1$.

Discussion & conclusion: The tradeoff between tolerable loss and depolarizing rates shown in Fig. 3 is consistent with the observations of Ref. [11]. Specifically, loss-specific codes aim to maximize loss-tolerance, while ignoring the effects of depolarizing noise. This can only be achieved by sitting near the $p = 0$ extremity of the bound. Therefore such codes will exhibit poor tolerance against depolarizing noise, heavily limiting their applicability. The converse also holds. Namely, conventional QECC's that specifically target unlocated depolarizing noise while ignoring qubit loss sit near the $\varepsilon = 0$ axis and therefore exhibit suboptimal loss tolerance. Note that we use the term 'suboptimal' as opposed to 'poor' in this context, because a code protecting against unlocated errors can automatically protect against as many located errors as unlocated errors. That is, located errors can always be trivially mapped to unlocated errors by simply not using the extra classical information during the recovery operation. Thus, any code protecting against t unlocated errors automatically exhibits the suboptimal tradeoff curve defined by $t_l + t_u \leq t$. Thus, this represents a trivial lower bound on loss/error tradeoffs. Note that the converse does not hold. Namely, unlocated errors cannot be trivially mapped to located errors.

In practise, useful codes will need to be tailored to sit in an intermediate region between these extremes to achieve acceptable levels of tolerance against both types of noise. Our results indicate that, at best, a roughly linear tradeoff between the two is possible. A linear tradeoff is quite optimistic and implies the potential existence of codes with good degrees of tolerance against both error types. The optimal tradeoff between the two will depend on the physical system. For example, in some architectures, such as solid-state systems, loss rates will inherently be very low, while in others, such as optical systems, they will be much higher.

Importantly, because existing loss-specific codes are designed with only loss-tolerance in mind, they are unlikely to be able to efficiently trade away loss tolerance for tolerance against depolarizing noise. For example, numerical investigations of the Ralph et al. [9] loss code indicate that the tradeoff curve of is restricted to the $p \approx 0$ region. That is, we are unable to move to an intermediate region which exhibits acceptable tolerance against both types of error.

It is already known how to construct QECC's that saturate the original quantum Hamming bound. An interesting research project would be to establish whether the generalized bound presented can be saturated, and if so to construct a class of codes doing this. Ideally such codes would allow us to sit at arbitrary points on the optimal tradeoff frontier and therefore be applicable to arbitrary physical systems with different inherent loss and noise characteristics.

The model we have presented has several inherent limitations. In addition to being restricted to non-degenerate codes, our model makes another implicit assumption about the behavior of codes – we assume the ability of codes to recover from errors is bounded by the number of errors that occur, but is independent of their location. This may seem like a very reasonable assumption – intuitively we might expect that good codes would exhibit this kind of symmetry. Interestingly, some recent loss-tolerant codes do *not* exhibit this property. For example, the ability of the Ralph et. al [9] parity state and Varnava et. al [10] loss-tolerant cluster state schemes to recover from losses are highly dependent on the configuration of loss errors. For a given number of losses, these codes may or may not successfully recover, depending on their locations. In both cases, this property owes to the inherent asymmetrical structure of these codes.

We have considered a general class of non-degenerate QECC's which jointly protect against depolarizing noise and loss. We studied the tradeoff between the number of depolarizing and loss errors a code can recover from. We then considered how this result translates into tolerable error and loss probabilities. Our results are consistent with recent results indicating that high loss-tolerance can only be achieved at the expense of tolerance against depolarizing noise. The converse also holds. However our results also indicate that, at best, a roughly linear trade-off between the two is possible. This suggests the possible existence of codes which jointly protect against both kinds of error without suffering drastic reductions in tolerable error rates. Should such codes exist, they would be much more useful in practical scenarios than specialized codes that target particular error types.

Acknowledgments

We thank Henry Haselgrove for providing helpful feedback and drawing our attention to an error in the initial bound. We also thank Tim Ralph, Bill Munro, Michael Nielsen and Alastair Kay for helpful discussions and feedback. This work was supported by the Australian Research Council and Queensland State Government. We acknowledge partial support by the DTO-funded U.S. Army Research Office Contract No. W911NF-05-0397.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] E. Knill, Nature (London) **434**, 30 (2005).
[3] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[4] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[5] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (96).
[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (97).
[7] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[8] P. Kok, W. J. Munro, T. C. Ralph, J. P. Dowling, and G. J. Milburn (2005), quant-ph/0512071.
[9] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).
[10] M. Varnava, D. E. Browne, and T. Rudolph (2005), quant-ph/0507036.
[11] P. P. Rohde, T. C. Ralph, and W. J. Munro (2006), quant-ph/0603130.
[12] E. Knill (2006), quant-ph/0312190.
[13] Qubit loss may be considered a located depolarizing error. Loss is located because we can use a quantum non-demolition (QND) measurement to non-destructively test for the presence of the qubit. Such a measurement can be understood in terms of its measurement projectors $\{|vac\rangle\langle vac|, |0\rangle\langle 0| + |1\rangle\langle 1|\}$, where $|vac\rangle$ represents the vacuum state. Thus, the measurement projectively determines whether the qubit is present or not, but in the logical Hilbert space performs the identity operation. Furthermore, loss is equivalent to depolarization because when a qubit is lost, so is all associated quantum information, as per depolarization.
[14] Notice that we include the identity component in the case of located errors, but not in the case of unlocated errors. This is because for unlocated errors we sum over all error configurations acting on up to t_u qubits. Thus, including the identity term would double count those configurations. However, in the case of located errors the number of affected qubits is fixed. Thus, the identity component of the depolarizing process must be explicitly counted.
[15] The no-cloning theorem states that for an arbitrary unknown state $|\psi\rangle$, it is impossible to perform the transformation $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$, i.e. to make two identical copies of the state. To see how this relates to the number of located errors one can correct for, consider the following. Suppose we encode a single logical qubit into an n qubit codeword. If we divide the codeword in two and give each half to a different party, both parties would be able to reproduce the original codeword if they could correct $n/2$ or more located errors, since they are both missing half their qubits. Thus, for $k = 1$, $t_l \leq (n-1)/2$. For $k > 1$, consider the following. Suppose our encoding operation maps the first $k-1$ logical qubits to the first $k-1$ codeword qubits directly, and the remaining logical qubit to the remaining $n-k+1$ codeword qubits. This strategy maximizes our ability to correct errors on the last logical qubit, assuming a unitary encoding operation. Now if $t_l \geq (n-k+1)/2$ we could clone the last logical qubit. Thus, $t_l \leq (n-k)/2$.
[16] The process characterizing the depolarizing channel is of the form $\mathcal{E}(\hat{\rho}) = (1-p)\hat{\rho} + p/3(\hat{X}\hat{\rho}\hat{X} + \hat{Y}\hat{\rho}\hat{Y} + \hat{Z}\hat{\rho}\hat{Z})$.